Incident Management Obligations

|  |  |
| --- | --- |
| Document filename: | **Incident Management Obligations**  |
| Project | **Service Management Standard** | Status | **Published** |
| Owner | **Live Services Primary Care Team** | Version | **3.1** |
| Author | **Service Management** | Version issue date | **27/11/2023** |

**Contents**

[Introduction 4](#_Toc130304388)

[General 4](#_Toc130304389)

[Resolution time measurement 4](#_Toc130304390)

[Incident & Service Request Logging 5](#_Toc130304391)

[Data correction 5](#_Toc130304392)

[Severity Level Framework 5](#_Toc130304393)

[Incident Severity Level definition 5](#_Toc130304394)

[Severity Level Guidance 7](#_Toc130304395)

[High Severity Service Incident 8](#_Toc130304396)

[Incident re-occurrence 9](#_Toc130304397)

[Supplier’s Service Management Tool/Online Portal 9](#_Toc130304398)

[Technical Security & Information Governance Issues 9](#_Toc130304399)

[External Incident notifications 9](#_Toc130304400)

[HSSI Report 10](#_Toc130304401)

[Minimum Data Set 10](#_Toc130304402)

# Introduction

This document provides direction to the Supplier with regard to the assessment and allocation of Severity Levels to Incidents. The requirements and obligations set out in this document apply to both Type 1 and Type 2 Catalogue Solutions.

This document forms part of the Service Management Standard.

The Catalogue Authority reserves the right to change, update and re-issue this document to suppliers by following the mechanisms referred to in clause 21 of the Catalogue Agreement.

In the event that the Supplier is unsure or unclear of any aspect of the content or interpretation of this document then the Supplier must contact the Service Management Agent for clarification.

Unless defined herein, capitalised terms in this document shall have the meanings ascribed to them in the Catalogue Agreement, Framework Agreement, Service Management Standard or ITIL V4 (or successor) in that order of precedence.

## General

The Supplier must manage Incidents in accordance with good industry practice.

Where an Incident is reported to the Supplier by another supplier or via the National Service Desk (NSD), the Supplier shall (in the Supplier's Incident log) record the reporting party's Incident log number. The Supplier will review the relevant report and if it agrees that an Incident has occurred (and that responsibility properly sits with the Supplier) then it will determine the appropriate Severity Level in accordance with the process set out above and, in respect of any HSSI, the Supplier will update the reporting party on a regular basis until the relevant Incident has been Resolved.

The receiving supplier is responsible for accepting and logging the Incident from the referring supplier subject to such acceptance and logging meeting the relevant supplier’s Minimum Data Set. The Supplier is responsible for the timely referral of Incidents which it determines are the responsibility of another supplier to the appropriate Service Desk of the relevant supplier(s).

The Supplier shall ensure that appropriate monitoring is in effect in respect of the Services it is providing. In the event of an Incident not being raised, the Supplier shall raise a retrospective Incident as soon as they become aware of the relevant Incident.

The Supplier is permitted to link Incidents if multiple Incidents are reported for the same issue, in accordance with good industry practice.

## Resolution time measurement

The Resolution Time of Severity Level 1 and 2 Incidents shall be measured continuously throughout Core Hours and Non-Core Hours.

Incidents lower than Severity Level 2 are only measured during Core Hours.

In relation to Incidents with a Severity Level lower than 2, in the event that the Supplier became aware of the Incident in Non-Core Hours, the Resolution time of the Incident shall only start to be measured when Core Hours next recommence. In the same circumstances, the Resolution time of Severity Level 1 or 2 Incidents would start as soon as the Supplier became aware of the same.

The Supplier is responsible for the referral of Incidents to their clinical safety officer which require clinical assessment no later than 2 hours from submission. Resolution Time for such Incident is measured from time of submission until the Incident is Resolved.

## Incident & Service Request Logging

For the avoidance of doubt, a Service Request is where the End User is specifically requesting help or guidance with performing a task. If an End User is reporting an issue with the Catalogue Solution or reporting that the Service is not working as expected, then this is an Incident.

All Offered Calls made to the Supplier shall be logged and classified as either an Incident or Service Request and must be reported as such.

## Data correction

If an Incident arises that results in the need for corrective action to be undertaken on data held within another supplier’s system, then where the Supplier has deemed this appropriate and the other supplier is governed by the Catalogue Agreement and the Framework Agreement, the supplier that provided the Defective Data that needs correcting shall be responsible for undertaking the necessary corrections (and any receiving suppliers shall co-operate and provide reasonable support in respect of any such corrective activities).

Where the Incident is deemed (by the Supplier) to have (or is reasonably likely to have) a material clinical or IG impact and there is a consequence or possibility of the data transferring between suppliers (being themselves subject to the terms of the Catalogue Agreement and related standards), then the supplier that provided the Defective Data must contact such downstream supplier(s) and transfer ownership or work in partnership with that downstream supplier to resolve. Please note the supplier that provided the Defective Data shall still be deemed responsible unless ownership transfer is agreed with another supplier. All suppliers (including the Supplier) must cooperate and support corrective and reconciliation activities as reasonably required.

# Severity Level Framework

## Incident Severity Level definition

The Supplier shall utilise Incident severity level guidelines for each of their Catalogue Solutions which align to the Incident Severity Level descriptions set out in the table below (where 1 is the highest Severity Level) and which are appropriate to the Supplier’s scale of Service Recipients and technical architecture. The Supplier shall provide their proposed Incident severity level guidelines for severity 3,4 and 5 to the Service Management Agent for review and approval (such approval not to be unreasonably withheld) via the standard compliance testing regime as conducted in accordance with the stage 3 of the Catalogue Onboarding Process ancillary document.

|  |  |
| --- | --- |
| **Severity Level** | **Description** *(Your responsibilities include but are not limited to the below)* |
| **1** | The Incident falls within the scope of one or more of the following:* >5% or more practices across the estate or Domain/Component System or equivalent where the Incident will, or is highly likely to, result in a material disruption to the Catalogue Solution provided to Service Recipients and/or Consumer Suppliers (for example, due to a significant loss of availability such as the following which is not an exhaustive list)
	+ Outage of any key module e.g. Appointment Management, Referral Management, Resource Management, Patient Information Maintenance -GP, Prescribing, Recording Consultations - GP *(Please note this is not an exclusive list)*
	+ Loss of Data Centre
	+ IM1 Bulk Extracts (howsoever provided) failure/corrupt data including rebulks fails for 2 consecutive days.
	+ Other IM1 API’s experience complete loss of service.
	+ A Spine Service unavailable e.g. GP2GP, SCR, EPS *(Please note this is not an exclusive list)*

and/or* the Incident is classified with a clinical risk rating of 5 (in accordance with the DCB0129 guidance);
* the Incident will, or is highly likely to, result in a material security breach and/or a material breach of the information governance provisions.
 |
| **2** | The Incident falls within the scope of one or more of the following:* >5% or more practices across the estate or Domain/Component System or equivalent where the Incident will or is highly likely to, result in a material disruption to the Catalogue Solution provided to Service Recipients and/or Consumer Suppliers (for example, materially reduced system responsiveness);
	+ IM1 Bulk Extracts (howsoever provided) failure/corrupt data including rebulks
	+ IM1 API’s degraded service

 and/or* the Incident is classified with a clinical risk rating of 4 (in accordance with the DCB0129 guidance);
* Either the ITSM Toolset, email and/or phone is unavailable
 |
| **Lower than 2** | Allocation of Incident Severity Levels below 2 are for determination by the Supplier (acting reasonably) and shall not be subject to compliance testing by the Service Management Agent. |

## Severity Level Guidance

A Severity Level is based upon **Distribution** and **Impact** of an issue and shall be consistently applied.

* **Distribution** is determined by the number of Service Recipients that are affected.
* **Impact** is determined based on the Catalogue Solution that is affected being whether it is a Type 1 Catalogue Solution or Type 2 Catalogue Solution and then calculated based on the impact (whether the Catalogue Solution is Available or Unavailable)

### Distribution

Distribution is determined by the number of Service Recipients and/or End Users actually or potentially affected by an Incident.

End Users may be considered to be potentially affected by an Incident whether or not such End Users are actually affected.

All Service Recipients and/or End Users will be deemed to be either actually or potentially affected by an Incident unless the Supplier can provide evidence that this was not the case as detailed below (the Evidence).

For the avoidance of doubt, the Evidence must detail the following:

1. Service Recipients and/or End Users that have either been actually or potentially affected; and
2. Service Recipients and/or End Users that have not been actually or potentially affected; and
3. Any Service Recipients and/or End Users that cannot be affected (the "Distribution condition"). Evidence can also detail which Service recipients cannot be impacted.

For the avoidance of doubt, the Supplier simply providing lists of Service Recipients and/or End Users falling into the above categories shall not be considered Evidence. The Supplier must provide full written detail as to how and why Service Recipients and/or End Users fall into such categories.

The Authority, acting reasonably, shall have the sole right to refuse to accept the Evidence provided by the Supplier.

An example of a scenario when End Users are potentially affected is set out below:

An End User is able to login into the NHS App or any other patient facing service app but that End User is unable to either view their patient record, unable order a repeat prescription, and/or cancel/book GP appointment (an Incident). It shall be deemed that all End Users are potentially affected by this Incident whether or not End Users actually attempt to view their patient record, order a repeat prescription or cancel/book a GP appointment unless the Supplier can provide Evidence that this was not the case to the reasonable satisfaction of the Authority.

When determining the number of Service Recipients and/or End Users that are potentially affected, the Supplier may, acting in good faith, calculate the number based on the information readily available to them and their experience of similar Incidents based always on the Evidence.

End User means a person using a Supplier’s Catalogue Solution (including any patient facing service).

In applying the Distribution condition, the following distribution classifications are used:

|  |  |
| --- | --- |
| Level | Distribution |
| High | Impacts or potentially impacts more >5% of Service Recipients that use the affected Catalogue Solution. |
| Medium | Affects or potentially affects between 5 Service Recipients or up to 5% of Service Recipients using the affected Catalogue Solution. |
| Low | Localised to affecting or potentially impacting 1 or <5 Service Recipients. |
| Very Low | Only affecting or potentially impacting a single End User at a Service Recipient.  |

### Impact

Impact is split into three categories: **1) Unavailable**, **2) Service Degraded and 3) Non-Performance Issue**, for which a description of each is detailed in the table below:

|  |  |
| --- | --- |
| Categories | Description |
| Unavailable | This is as defined as a Catalogue Solution is Unavailable to a Service Recipient. |
| Degraded | The Catalogue Solution can still be accessed by Service Recipient(s) and will perform the intended task successfully. However, timescales to complete the task are longer than expected or the Catalogue Solution performs with unexpected behaviour. This includes (but is not limited to) data issues where data is inaccurate.  |
| Non-Performance issue | The impact of the Incident / Problem does not fall into either of the above categories. For example the impact is not related to the usability of the Catalogue Solution, rather it relates to the overall aesthetic of the system such as a typo. |

### Severity Level Matrix

Based on the Distribution and Impact levels presented above, the following matrix will be used for the assessment and allocation of severity levels.

|  |
| --- |
| **Impact** |
| **Distribution** | **Unavailable** | **Performance Degraded** | **Non-Performance Issue** |
| **High** | Severity 1 | Severity 2 | Severity 3 |
| **Medium** | Severity 2 | Severity 3 | Severity 4 |
| **Low** | Severity 3 | Severity 4 | Severity 4 |
| **Very Low** | Severity 4 | Severity 5 | Severity 5 |

### Clinical Safety Issues

Incidents with a Clinical Safety Rating must be assessed as per DCB0129 implementation guidance risk estimation. If the Incident has been given a Clinical Safety Rating, then the following Severity Levels shall be applied.

Where the resultant Clinical Safety assessment of risk (as set out in DCB0129) differs from the Incident Severity Level Matrix then the Severity that is higher shall be used.

|  |  |
| --- | --- |
| **Clinical Safety Assessment of Risk** (as per DCB0129) | **Incident Severity** |
| 5 | Severity 1 |
| 4  | Severity 2 |
| 3  | Severity 3 |
| 2  | Severity 4 |
| 1 | Severity 5 |

# High Severity Service Incident

Any Incident (including any linked Incidents) where the Severity Level is classified by the Supplier as either Severity Level 1 or Severity Level 2 shall be treated and logged as a High Severity Service Incident (each an “**HSSI**”).

The Supplier shall report all HSSIs by phone to the Service Management Agent’s Service Bridge within 20 minutes of identification. By agreement between the Supplier and the Service Management Agent (acting reasonably), the Supplier may report HSSIs in an electronic form on the basis that the data required in the HSSI notification meets the Service Management Agent’s minimum data set requirements as set out below.

## Incident re-occurrence

If after a Severity 1 or 2 Incident has been held to be Resolved, it is later established that the relevant Incident was not actually Resolved or the same Incident reoccurs within 3 (three) hours of being originally Resolved, then the relevant Incident will be deemed not to have been Resolved in the first place and the Resolution Time of the Incident will be deemed to be ongoing (from the time that the relevant Incident is held to either not have been Resolved or it reoccurs) until the Incident is actually Resolved. The Resolution Time measurement will include the time period that the Incident was temporarily Resolved and/or the time period that the Supplier believed that the Incident was Resolved (as the case may be).

## Supplier’s Service Management Tool/Online Portal

Any unavailability (partial or wholly) of the Supplier’s Service Management Tool/Online Portal or telephony system shall be classified as a Severity 2 Incident.

## Technical Security & Information Governance Issues

Actual or potential Technical Security and / or Information Governance related Incidents must be raised as a HSSI regardless of distribution and impact.

Technical Security and Information Governance issues include but are not limited to: the protection of information and information systems from unauthorised: (i) access, (ii) use, (iii) disclosure, (iv) disruption, (v) modification, or (vi) destruction, or any other issue that would amount to a breach of the applicable data protection legislation.

## External Incident notifications

With the objective of facilitating the effective management of service disruptions across the NHS:

1. Where the Supplier becomes aware of a material incident that is not due to an issue with the services, they provide but is potentially due to a service that the Service Management Agent has oversight of or contracts for, the Supplier shall notify the Service Management Agent’s Service Bridge of the relevant incident.
2. Where the Service Management Agent becomes aware of a material incident that potentially has a material impact on the Service Recipients of the Supplier, the Service Management Agent shall notify the Supplier of the incident and shall keep it appraised of progress with resolution.
3. Where the Service Management Agent determines, acting reasonably, that the Supplier can contribute to the resolution of a material incident that is not directly attributable to an issue with the Supplier’s services, the Supplier shall participate in multi-supplier calls in order to support the determination of incident allocation and/or resolution.

## HSSI Report

Upon closing an HSSI, the Supplier must complete the embedded HSSI Report below and send it to the Service Management Agent within 5 Working Days of the closure date of the HSSI.

By agreement between the Supplier and the Service Management Agent (acting reasonably), the Supplier may provide the content of HSSI Reports in an alternative electronic form on the basis that the data required in the HSSI Report is provided in such alternative.



## Minimum Data Set

### Initial notification

Suppliers must report HSSIs to the NHS England Service Bridge on 0113 397 3973 – (24/7). When reporting the HSSI, the following minimum data set must be provided:

* **Suppliers Reference Number:** The incident reference number used by the supplier’s Incident Management tool.
* **The Time Incident occurred:** The time the Supplier confirm the commencement time of the incident
* **Severity:** Is the Incident Severity 1 or Severity 2
* **The service / product affected:** The service or services impacted
* **Description:** Description of the incident as experienced at the time according to the MDS.
	+ *How the incident was detected (reported by user / monitoring alerted us etc*
	+ *Description of the component at fault.* – *as the Supplier recognise it at this stage (if available)*
	+ *Potential linked HSSIs (if a link can be made)*
	+ *Details of symptoms and Initial diagnosis*
	+ *Details of any workarounds or alternative working practices available (if available)*
	+ *Will the Supplier be attempting to replicate the issue (if known)*
	+ *Number of users affected (if known)*
* **Impact:**What is the current known impact to the user(s). Any Clinical / Cyber Security / Information Governance implications/impact/risk.
* **Agree** next update time based on Severity
* ***Conference Calls -*** *Based on the severity and type of incident the Supplier maybe asked to join a NHS England Service Bridge Conference Call at short notice. The NHS England Service Bridge will chair and formalise a call with the relevant Supplier & NHS England parties present. This will replace the formal update process as feedback will be taken on the calls.*
* ***Severity 1 & 2 Guidelines***

 **Severity 1**

* + Initial call – within 20 minutes
	+ 1st update – 1 hour
	+ Following updates – Every hour until resolved

 **Severity 2**

* + Initial call – within 20 minutes
	+ Following updates – Every 1.5 hours until resolved

### Additional updates during the HSSI lifecycle

**The service / product affected Update:** The Supplier (Major Incident Manager) MIM should provide the NHS England Service Bridge with a detailed progress update before or on a time agreed when the incident was first raised.

**Impact Update**

* Has the Impact changed? Is it more or less significant than first though

**Diagnosis Update:**

* Description of the component at fault – what is known at this point
* Is there any update on details of any workarounds or alternative working practices available
* Has the incident symptoms been replicated by the supplier and what have investigations so far shown

**Further Updates**

* What further diagnostics has the Supplier tried – what steps have been taken so far – any ETA’s
* Provide updates on any further information requests which NHS England have requested. N.B. If the NHS England Service Bridge request further info, the SUPPLIER should endeavour to gather this information and NHS England should be expected to clarify the reasons for needing this information if the Supplier MIM requires. This is so the MIM can articulate the request and the need for the information to the Technical Teams/SDMs.
* Attend Conference calls if invited by NHS England Service Bridge